# Broad Agency Announcement Solicitation/Call: HSHQDC-17-R-00030
# Project: Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT)
# Research and Development (R&D)

This BAA solicitation/Call (HSHQDC-17-R-00030) is a Call issued against Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year Broad Agency Announcement (BAA), HSHQDC-17-R-B0002 (current issue). All terms and conditions of the DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue) apply to this solicitation unless otherwise noted herein. The "current issue" of the DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 used herein refers to the latest issue posted in Federal Business Opportunities (FBO).

## 1. Introduction:

Empirical data and productive analytics are fundamental to high quality cybersecurity research and development (R&D). Cybersecurity Research and Development (R&D) requires these foundational elements to develop advanced knowledge, and to accelerate design, production, and evaluation of next-generation cybersecurity solutions. However, the value of having a research infrastructure that enables real-world, large scale, and longitudinal data collection, provisioning, and analysis to the R&D community is severely underestimated; too often such an infrastructure is assumed to exist without deliberate resource affordances[1]. DHS/S&T/CSD has uniquely championed this R&D resource via the IMPACT project (Information Marketplace for Policy and Analysis of Cyber-risk & Trust) (https://www.impactcybertrust.org)[2].

IMPACT enables, sustains, and mediates the provisioning of freely available cybersecurity data and analysis, between providers and seekers, within the global industrial, academic, and government cybersecurity communities [3]. It lowers the barrier to entry for cybersecurity R&D by addressing the operational, legal, and administrative costs that otherwise impede scalable and sustainable data sharing needed to enable higher quality cybersecurity R&D innovation in a responsible manner. IMPACT reduces the time and cost associated with finding, curating, and acquiring data in a manner that is mindful of the associated legal and ethical risks. IMPACT also supports DHS/S&T bilateral agreements and makes its data available to approved international locations.

*Data repositories exist today, but many are unable to deal with proliferation of massive data sets, do not support semantically rich data searches and have limited data provenance information … [s]tatic repositories are of limited value for resilience research, where dynamic, agile repositories are needed … [r]esearch in cybersecurity requires realistic experimental data which emulates insider threat, external adversary activities, and defensive behavior, in terms of both technological systems and human decision making. The integrity and availability of such data sets is crucial to ensuring scientifically reliable results …There is a substantial lack of vetted, provenance -detailed, and openly available data sets that are needed in order to obtain research reproducibility, an inherent trait of the science of security. Special, one-off relationships with industry partners to acquire access to their proprietary data means that a broader pool of researchers cannot utilize the data or peer review the results … Cyber-threat data sharing for operational purposes is crucial in the defense against malicious cyber activities. Such data sharing also has vital strategic benefits to enable research of new, effective ways to protect critical information systems. Currently, data owners possessing real, high-fidelity data are reluctant to share such data for government-funded research. Data* *owners take on risk when sharing their data with researchers —disclosures of events could damage their reputation and impact business or the public [4].*

The IMPACT project components that address these core R&D infrastructure requirements include metadata discovery, data matchmaking, and trusted mediation of data sharing to legitimate researchers. [5] IMPACT's first generation R&D-enabling infrastructure (PREDICT) focused on democratizing *data raw materials* for the cybersecurity community. This BAA call intends to foster an evolved IMPACT R&D infrastructure that, in addition to enabling raw materials, will now democratize *derivative data products and tools* for Homeland Security Enterprise (HSE) [6] decision analytics [7]. This additional component directly responds to the developing challenges in the stewardship of large-scale, longitudinal and real-time, heterogeneous, multidimensional, and/or dynamic data and analytics. Such an augmented foundation is needed to empower advances in cybersecurity R&D that are required to withstand and surmount persistent and evolving threats [8]. Specifically, this BAA seeks to foster the transitioning of complex data and analytics into practical and effective cybersecurity decisions by supporting derivative data, tools, and analytic techniques that are directly responsive to the decision needs required to manage cyber risk to the HSE.

## 2. Description and Scope:

Existing capabilities do not currently provide the necessary risk analysis, risk management, and decision making support needed by enterprise owners and operators across the Federal Government, critical infrastructure, and private sectors [9]. Decision analytic capabilities are needed to support a more integrated, holistic understanding of the risk environment and strategic needs to enable effective interventions in the form of investment and other activities to prevent, protect, mitigate, and recover from cyber disruptions and harm [10]. Achieving targeted and timely decision making necessitates empirical data and analytic tools that are responsive to the cybersecurity challenge at hand, and that abstract the irrelevant complexities that typically impede cognition and decisive action. Responsible R&D also demands that these data and analyses are transparent and capable of provenance proofing [11].

To meet this need, DHS/S&T has initiated the IMPACT project (a diagram of the evolved IMPACT project is enclosed in *Appendix A*. Performers consist of Data Providers (DPs) and Data-Analytics-as-a-Service Providers (DASPs), which correspond to the *Data* and *Application* layers, respectively. These entities will work independently and/or in concert to provision data and analytic tools using the IMPACT infrastructure, which will continue to mediate between providers and seekers of data and analytics. Offerors of DPs and DASPs should discuss how they will address the target customers' decision needs (*Inputs)* by specifying the Cyber Security Challenge Problem(s) (CCP) they will target, and by providing the associated data and analytic capabilities to enable one or more *Outcomes* illustrated in the *Introduction*.

This next phase IMPACT program addresses the quantitative and qualitative requirements for the cybersecurity decision analytic needs of HSE target customers in the face of high volume, high-velocity, high-variety, and/or high-value data. *Decison analytics* is defined here as a service technology or tool capable of supporting the following typeof analytics: descriptive (what happened); diagnostic (why it happened); predictive (what will happen); and prescriptive (what should happen). In general, decision analytic requirements comprise the following:

- Integrated and scalable risk-assessment and risk-management capabilities, technologies, and methods to support secure and resilient infrastructure [12];
- Identification and characterization of cyber-logical and cyber physical, cross-domain, economic, behavioral, societal, and environmental data;
- Verifiable and validated analytics for use in risk-assessment methodologies and standards of practice for their application;
- Data science for cybersecurity that characterizes the challenges, implications, and opportunities presented by the increasingly distributed, complex, and richly connected critical infrastructure environments; describes the architectures and requirements of integrated data acquisition networks and intelligent systems for enhanced situational awareness; informs criteria and standards for broad-scale data acquisition; and conveys ontology and topology frameworks for sharing data across domains [13].
- Access to information and communication technology (ICT) data sources for cybersecurity R&D purposes. Currently available data lack comprehensive coverage, are difficult to integrate across disparate sources, are riddled with significant noise in various forms, and/or lack normalization between and across disparate sources [14].

## 3. Technical Topic Areas (TTAs):

This BAA call intends to stimulate the transition of research to practice [15] by stewarding an evolved R&D-enabling infrastructure that more directly addresses the data and analytical needs of the cybersecurity R&D community and the HSE [16]. Specifically, there is a growing need for dynamic and responsible R&D to support decisional needs of the HSE. These needs can be broadly categorized as situational awareness, decision support and optimization, risk modeling & analysis, economic analysis, statistical analysis and scoring, modeling and simulation [17]. They can be addressed with advanced operational research infrastructure that is responsive to the data and analytic requirements to support cyber risk decisions in a responsible manner [18]. Non-exhaustive examples of the types of *Outcomes* that this BAA call will support include:

- Real-time network event identification and monitoring: examine and analyze data from multiple sources for identification of unique and specific cybersecurity events; review key events surrounding natural, adversarial or accidental situations to determine the extent or potential of threats, incidents and/or hazards

- On-demand measurements and experimentation: continuously query for streaming applications such as traffic analysis or ad-hoc network forensic investigation (e.g., outage detection such as cable cuts or natural disasters; Border Gateway Protocol hijacks)

- Time series analyses: coalesce signals/observed patterns over time to detect correlations and evolving and emerging threats; compress long durations of events/activities into more concise digests, to easily view an index of all events in a given instance/time-period/geography

- Event reconstruction: correlate data across multiple different sources via visual and non-numeric analytics to offer insights (forecasting/predicting) and responsiveness to complex events; provide longitudinal and historic optics to confirm suspected cybersecurity event

- Tactical and strategic resource allocation in support of cyber resilience: assess real-world security and stability properties such as hygiene, robustness, resilience, and economic sustainability

- Analytic frameworks that characterize adaptive cyber adversary attacks and associated likelihoods and severity of consequences

- Identification of cyber interdependencies, aggregation risk, and cascading harm

- Risk management: model, score and evaluate component and systemic cyber risk (including prediction of risk of action or inaction) to support effective courses of action and investments in cybersecurity controls

- Evidence-based, reproducible data and analytics to inform communication technology policy.

To support performance measurement, Offerors will need to supply metrics aimed at measuring ongoing utility and management of the data and/or tools they intend to make available under this BAA Call.

### TTA #1: Data Providers (DPs) Network

TTA 1 (as depicted in *Appendix A*) seeks to provide foundational data hosting and provisioning to fulfill the IMPACT project objectives. Using the IMPACT infrastructure [19]. Each Data Provider will provide the data that it owns or has a right to control and disclose to researchers, and also maintain the computing infrastructure to store and distribute data it receives or collects. To support the evaluation of next-generation cybersecurity solutions, using the IMPACT mediation infrastructure, IMPACT DPs will make cybersecurity research data available to the international research community.

Specific to TTA #1, DHS is seeking DPs to make available, subject to IMPACT terms and conditions, the following non-inclusive *categories* of data that are relevant to cybersecurity R&D: hostile/malicious activities (e.g., malware, phishing, botnet, data breach, insider threat, other cybercrime measurements), Internet demographics (e.g., network naming and routing, ISP interconnection data, physical and logical Internet and network representations), wireless and cellular network, cyber physical systems (e.g., power grid, Internet of Things (IoT))[20]. In addition to the examples above, other *types* of data may include but are not limited to: address space allocation, Border Gateway Protocol (BGP) routing, black-hole address space, labeled traffic traces, scan data, intrusion detection system (IDS) and firewall, infrastructure, Internet topology, Internet protocol (IP) packet headers, performance and quality measurements, synthetically-generated attacks, unsolicited bulk email, traffic flow, and botnet command and control traffic. Offerors may propose to engage other types of cybersecurity data; however, all technical approaches should describe the cybersecurity relevance of the data to be provided, as well as any associated terms and conditioned that would have to be administered by the IMPACT mediation infrastructure.

**3.1.1 Goal #1:** Describe the types of data the offeror intends to make available and the rationale for how that data supports one or more decision analytic needs of HSE target customers, described in Section 1 *Outcomes*, and/or one or more cybersecurity challenge problems (CCP) outlined in 3.2.1. Offeror should describe, to the extent feasible, metadata related to the volume, velocity, quality, availability, privacy-preserving measures/encodings, integrity schemes, and suggested sampling rates of the data it will make available.

**3.1.2 Goal #2:** Design and demonstrate data collection, curation, hosting and provisioning capabilities. Offeror should describe the intended storage and provisioning capabilities that support Goal #1. DPs will be expected to submit a collection, curation, hosting and provisioning capabilities design plan.

For example, what is the architecture and scale of the hosting infrastructure--is it self- or distributed hosting? What is the transmission/distribution model - will it support offline, longitudinal data or focus on dynamic, real-time data? Will data be accessible via computation on a remote data enclave, queries to interactive application, or via raw data download? In addition, the offeror should describe where the value of its capabilities lies, i.e., in the curation of volumes of relatively accessible "dirty" data and/or in the provisioning of unique data.

**3.1.3 Goal #3:** Provision data to DASP layer performers. As relevant, Offeror should describe any intended collaboration with DASPs described in Section 3.2 that supports data workflow reliability (i.e., coordination activity to package, stage and/or deliver data) in conjunction with DASP capabilities.

**3.1.4 Goal #4:** Provision data to IMPACT users via the IMPACT mediation infrastructure. Offeror should describe how it intends to measure, assess and evaluate the current and ongoing value of the data it provisions. For example, whether the data is directly responsive to requests made by researchers & developers, whether the data is expressly reactive to a recent cybersecurity challenge problem for which the community needs accessible data, or how Offeror will otherwise quantify the value of the data to the HSE and R&D community.

## 3.2 TTA #2: Decision Analytics-As-A-Service Providers (DASP) Network

TTA 2 comprises the IMPACT *Application* layer (as depicted in Appendix A). It will consist of a network of operational research environments that enable cybersecurity analysts, operators, and researchers & developers in industry, government and academia to reduce the amount of time and effort finding, curating and understanding data, so they have more time to extract insight and meaningful information to enhance their decision-making. The DASPs role is to abstract away the low level knowledge- and labor- intensive elements that comprise high dimensional data identification, complex association and fusion, and high-context presentation elements of data for decision analytics.

In general, DASPs are responsible for leveraging existing resources to enhance a data and analytical environment or standalone capability for the purpose of repeatedly and reliably providing storage and access to the decision analytics data and/or tools (e.g., visual analysis and awareness front end tools, analytics enabling tools, and/or algorithms). Brand-new build-out of infrastructure is not supported, however, enhancements to existing infrastructure to directly support proposed capabilities are permissible. Technical approaches to this TTA must present one or more cybersecurity challenge problems (CCP) and capabilities, and include reasoning as to how the proposal has the potential to address HSE decision analytical needs.

**3.2.1 Goal #1: Cyber Security Challenge Problems (CCP)**. Offerors should define and address one or more cybersecurity problem(s) that are mapped to or inferred from the decision analytic needs of HSE target customers, described in Section 1 *Outcomes*. These CCPs may also support other CSD Programs. [21] It is expected that each CCP should be separately costed except where offeror capabilities will address multiple, overlapping CCPs.

The classes of cybersecurity problems that a DASP Offeror should address include, but are not limited to:

a. Security, Integrity, Stability, Resilience of networks, Internet of Things, clouds (e.g., with respect to large-scale network events, and vulnerabilities)
b. Anti cyber crime economic incentives and interventions
c. Cybersecurity supply-chain resilience
d. Internet risk, and reputation scoring and validation
e. Threats, vulnerabilities, and hazards to critical infrastructures: telecommunications, transportation, logistics, commerce, life sciences, transportation, energy, environment.
f. External threat monitoring, mitigation, validation; including understanding the motivations behind emerging threats and potential attacks
g. Insider threat modeling and mitigation
h. Sensitive data sharing and controlled data disclosure (e.g., regarding vulnerabilities, threats, methods, strategies for coordinated cyber defense) [22]
i. Interdependencies, cascading, and aggregate effects of cyber-vulnerabilities and attacks across platforms and enterprises (Data and analytic methods or tools that inform about interdependencies and at what confidence levels; and improve analytic frameworks and risk models to enhance cyber resilience)

**3.2.2 Goal #2: DASP Performer Capabilities [23].** Performers are expected to augment or improve an Internet-accessible operational research environment or standalone leading-edge process, application, tool and/or technology and make it widely available to the cybersecurity R&D community (government, industry, academia) in order to support scientific, evidence-based advances in cybersecurity decisionmaking. DASP offerors should describe the type of and technical foundation for one or more capability they intend to demonstrate to support the CCPs that are targeted in Section 3.2.1. As well, Offeror should either describe how it envisions the stated capability(s) will advance knowledge of complex data storage, processing, and provisioning for cybersecurity R&D; or, articulate how the stated capability(s) will facilitate shared, scalable, and sustainable understanding of data science for cybersecurity. In either case, DASPs will be expected to submit a capability(s) design plan. Examples of the types of capabilities expected of DASPs include one or more of the following:

- Deploy a query-able online platform that supports rapid queries on datasets for research prototyping, including aggregating, synthesizing, annotating, enriching and presenting/delivering data from and across multiple data sources; and enhance the completeness, accuracy, and reliability of large-volume integrated data annotations.

- Demonstrate environments that visualize and provision high-volume data and analytics across distributed datasets (including geographic and virtual entities).

- Design and develop analytical frameworks that incorporate multiple analytic methods and techniques based on different architectures and technologies.

- Engage crowdsourcing as a distributed, complex analytic tool.

- Provide visual and/or textual streaming data analytics and applications for complex event processing (batch, cloud, edge, stream).

- Demonstrate advanced data disclosure control tool and/or service for provisioning of sensitive data while maintaining data utility.

- Enable the research and development of algorithms and methods for building analytic module (scorer) that provide a transparent risk scores and confidence levels.

- Provision a continuous query system (by providing a common query syntax, software infrastructure, and optimization framework for different types of analysis).

- Provide time-series comparisons and correlations to enable users to develop and test hypotheses.

- Develop analytical methods and computational models that consider socio-technical (e.g., behavioral economic) signals to uncover and predict threat and/or defender patterns.

- Enable risk-sensitive decision analytics by applying controls on the provisioned data and analytics that are proportional to any legal (privacy, confidentiality) and ethical risk.

- Demonstrate an experimental platform that integrates with an existing testbed to support experimental research (e.g., develop features that will enable different attack scenarios to be programmed and relevant data captured for subsequent analysis).

**3.2.3 Goal #3**: **Operational Research Capability Output.** DASPs are expected to demonstrate that targeted DASP data and analytical environment/tool capabilities have been achieved by making them available to researchers & developers via the IMPACT infrastructure. In addition, DASPs must demonstrate value by engaging actual users and providing objective metrics for the utility of the capability(s) being offered. Offeror should describe how it intends to measure, assess and evaluate the current and projected value of its undertaking in TTA #2. For example, whether it is directly responsive to requests made by target customers of this BAA, or whether it is expressly reactive to a recent cybersecurity challenge problem for which decision analytics are needed.

### 3.3 Exemplar of Challenge Problem, Capability, and Output

Research and develop data, techniques and methods to assist researchers and developers, and HSE targets to:

**3.3.1** Identify macroscopic Internet vulnerabilities. Identify structural vulnerabilities in the Internet topology that adversaries could target to block, disrupt, censor, or eavesdrop on Internet traffic. Specify key entities in the Internet ecosystem of a geographic region or critical infrastructure (e.g., communications, energy, transportation), map connectivity among them, and identify “critical points” in the topology. Create annotated Internet data and control-plane maps that improve the ability to identify, monitor, and model critical cyber-infrastructure.

**3.3.2** Reason and calculate (establish scoring and confidence level) projected impacts resulting from adversarial exploitation of Internet vulnerabilities. Develop vulnerability metrics that quantify the susceptibility of the Internet in a country/region to disruption by various types of adversaries. For example, if only a few autonomous systems (ASes) can transit traffic in/out of the country, this implies a vulnerability to AS-level adversaries, whereas if all paths in/out of a country traverse the same Internet exchange points (IXes) or terrestrial/submarine cables, then this would imply a vulnerability to attacks on the physical infrastructure.

**3.3.3** Model the effect of various avoidance and mitigation measures on projected impact. Estimate direct and indirect impact such as how much damage an attacker could cause by targeting the critical points in the Internet topology of a country. This could include quantity and quality of networks, users, traffic, or other resources that might be disrupted.

## 4. Project Structure

### 4.1 Project Status Deliverables

The following project status deliverables are required throughout the period of performance:

| DELIVERABLE | DUE DATE |
|---|---|
| Presentation Materials from Project Meetings | Within three (3) days of presentation |
| Triannual Technical Status Reports | Starting 120 days after award, and every 120 days thereafter throughout the base period of performance. For last 75 days of base period, report due 5 days prior to end of base period of performance. For each option period, report due every 365 days from effective date of option. |
| Monthly Financial Status Reports | Starting on the fifteen (15) day of the month, beginning in the calendar month after award, and the fifteen (15) day of each month thereafter throughout the period of performance. |
| Program Reviews | 3 and 5 months after award of the base period, and 4, 8 and 11 months after the exercise of each option thereafter. |
| Capability/Output/Deployment Reports | As may be required by the Government. The Government will return comments not later than fifteen (15) days after receipt. Performer shall submit updated document not later than fifteen (15) days after receipt of Government comments. Performer will provided updates and supplements to this document, as appropriate, during the period of performance. |

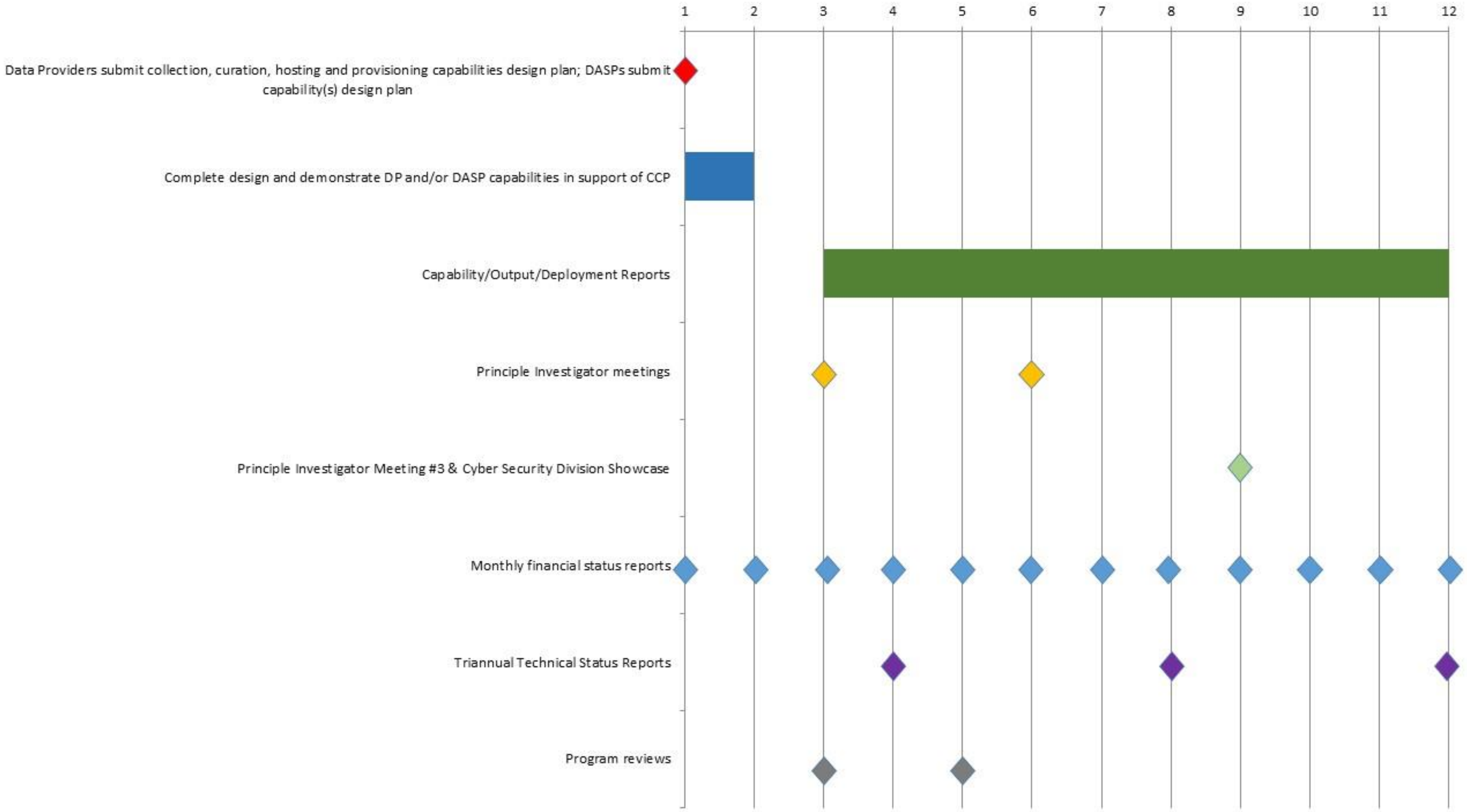
## 4.2 Key Technical Deliverables

The following key deliverables are required for each severable period of performance:

| DELIVERABLES | DUE DATE |
|---|---|
| Data Providers submit collection, curation, hosting and provisioning capabilities design plan; DASPs submit capability(s) design plan | 1 month after award |
| Complete design and demonstrate DP and/or DASP capabilities in support of CCP | 2 months after award |
| Principle Investigator Meeting #1 | 3 months after award |
| Principle Investigator Meeting #2 | 6 months after award |
| Principle Investigator Meeting #3 & Cyber Security Division Showcase | 9-12 months after award |
| Triannual Technical Status Reports | Starting 4 months after award |

## 5. Project Schedule/Milestones

A notional project schedule is shown below including anticipated milestones, meetings and demonstrations.



## 6. Special Instructions/Notifications

### 6.1 Response Dates

| Event | Time Due | Date Due |
|---|---|---|
| Industry Day | TBD | On or about February 23, 2017 |
| Proposals Due | 4:30 PM EST | March 24, 2017 |
| Notification of Proposal Selections | | May 1, 2017 |

### 6.2 General Instructions and Information

**6.2.1** This BAA solicitation/call (HSHQDC-17-R-00030) ***does not include a requirement for white papers*** and only requires the submission of proposals subject to the date identified in the "Response Dates" table above. Offerors should define and address one or more cybersecurity challenge problem(s) that are mapped to or inferred from the decision analytic needs of HSE target customers, described in Section 1 *Outcomes*. These CCPs may also support other CSD Programs. Proposals may address one or both technical topic areas. In all cases, the offeror shall propose to provide data and tools for release that are compliant with all laws and regulations that are pertinent to the data, and full compliance with the IMPACT legal framework (which includes international dissemination). Furthermore, the Government reserves the right to select one or more tasks per proposal and to select individual IMPACT data, decision analytics, and tool types for any task proposed. An overarching requirement of all DASPs and DPs is that they own or have a right to control and disclose to researchers the data they propose to make available, and that they will provide a legal and ethical risk assessment prior to making it available.

**6.2.2** Proposals must clearly state which of the two TTAs are being covered. If more than one TTA is being covered, then the submission must describe which of the TTAs is being addressed by the different aspects of the proposed work and clearly differentiate the tasks. This information is to be included along with the information required by DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002, (current issue) and Section 9.6.1.g, which outlines the requirements for "Detailed Technical Approach" for proposal submissions.

**6.2.3** Procedures for submission of proposals in the DHS S&T Portal are provided in paragraph 10 of DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current edition). Note that offerors must complete the company/organization portal registration PRIOR to submitting a white paper for the first time. Ensure adequate time to complete the company or organization's registration as delays in this process will not be authorization for late submissions of white papers. Company/organization registration information is located in paragraph 10.1 of DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current edition). In addition, each proposal requires registration in the portal. Information regarding proposal registration is located in paragraph 10.2 of DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current edition).

**6.2.4** Offerors may provide multiple proposal submissions; however, each submission must be distinct and self-contained without any dependencies on other work of any kind. Additionally, submissions, in either the white paper phase or proposal phase, that address a single TTA will be favored over expansive approaches that address more than one TTA. Therefore, offerors are discouraged from addressing more than one TTA per submission, unless there is a clearly complementary benefit that would yield an integrated result. Each submission must clearly state which TTA is being addressed.

**6.2.5** All software developed and delivered is required to be subject to security auditing; therefore, the offeror's technical approach must identify how security auditing will occur. Also, DHS expects offerors to follow best practices on software design and encourages the use of penetration testing to ensure functionality and security for all software deliverables.

**6.2.6** As stated in DHS S&T CSD BAA HSHQDC-17-R-B0002, DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to this BAA solicitation.

**6.2.7** The Evaluation Criteria in DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current edition) [3] Section 11 “EVALUATION OF WHITE PAPERS AND PROPOSALS” applies.

### 6.3 Foreign Participation

Offerors are reminded that foreign participation may occur as defined in DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue) Section 1.3. Therefore, offerors should provide unit costs for any deliverable not anticipated for delivery in a softcopy format.

### 6.4 Export Control Requirements

Offerors are reminded of the export control markings required by DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue) Section 8.6.8 (for white papers) and Section 9.6.4 (for proposals).

### 6.5 Type Classification Ceilings

Type classifications will not be used for this BAA call. However, DHS expects to make Individual awards with a 12-48 month period of performance and annual funding ranging from $100,000 to $600,000. Compelling proposals outside these parameters will be considered.

### 6.6 Travel

For purposes of estimating costs for white papers and proposals, offerors should anticipate travel to three program meetings per year, as described below.

**6.6.1** DHS Cyber Security Division holds an annual PI meeting where all DHS CSD funded efforts are expected to present. Projects will be required to provide a briefing, typically 20 minutes, and are required to provide demonstrations when appropriate. The PI meeting is typically 2.5 days.

**6.6.2** In addition to the annual DHS PI Meeting, the IMPACT Program will hold three program review meetings each year, one of which will coincide with the dates of the CSD annual PI meeting.  Meetings may be arranged by TTA and the meeting for each TTA is expected to last one day. When possible, TTA meetings will be held on adjacent days so funded efforts in one TTA can optionally attend other TTA meetings.

### 6.7 Proposal Requirements

To be considered for award, offerors MUST submit a proposal, compliant with the aforementioned response dates, in accordance with the DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue). Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue) may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count). The DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue) [3] Section 9 discusses proposal preparation and describes the required proposal content; however, in addition to the guidance in Section 9, the following special instructions are added:

**6.7.1** The maximum number of pages for Volume 1 is 25 pages.

**6.7.2** The information outlined below must also be included in any submitted proposal.

- **Proposed Use for DHS/S&T**: A detailed explanation of how the proposed output product(s) supports the targeted end user (e.g., the HSE) in an operational context. Include quantitative specifications for how the output product(s) will improve operational performance.

- **Operational Utility Assessment Plan**: A detailed plan for demonstrating and evaluating the operational effectiveness of the Offeror's products in exercises, including evaluation metrics. Explain your view of the requirements gap to be filled, what capability will be provided upon successful completion of the proposed effort, and what are the technical risks associated with successful maturation of the proposed effort to achieve operational utility. Explain your concept of how you will develop and demonstrate a system or system component. Identify and explain the critical path technologies or key technical challenges you will face when building this system or component and your plans for meeting these challenges. Explain how you will demonstrate the system or component performance relative to the performance or enhancement goals described in the proposal.

**6.7.3 Subcontractor Cost Submission:** Referencing, DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue), Section 9.6.2.b.(6), if the subcontractor costs cannot be included with a prime's detailed cost breakdown, then the prime contractor must stipulate on the detailed cost breakdown that the costs presented only represent those from the prime and the subcontractor's costs are provided separately as an attachment to an e-mail sent to CSD-2017-BAA@hq.dhs.gov. The subject line of the email shall say "Separate Subcontractor Cost Submission – [insert the proposal number assigned from the DHS S&T BAA Portal]". The body of the email shall contain the following:

1) The prime entities name which should be the same entity that is registered in the BAA portal;

2) A POC (name and phone number) from the prime entity; and

3) For each subcontractor proposal attached, include:

   - The name of the subcontractor for the subcontractor proposal attached; and
   - A POC (name and phone number) from the subcontractor whose proposal is attached.

The separate subcontractor cost proposal must be as detailed as the offeror's cost proposal and must be received at the location designated in the individual solicitation no later than the closing date and time specified by the solicitation. Note that email transmission time may vary depending on the file size of the attachment(s) included in the email. Therefore, ensure there is adequate time for receipt of the email and any accompanying attachments of the subcontractor(s) cost proposal(s) by the required closing date and time. Acceptance of the email submission is dependent upon the actual date and time the e-mail and any accompanying attachment(s) is RECEIVED by the in-box for CSD-2017-BAA@hq.dhs.gov. ***NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE.***

### 6.8 Link to Industry Day

An industry day for this solicitation will be held on or about February 23, 2017 in Washington, DC. Parties who are interested in participating in the industry day may register using the following link: http://www.cvent.com/d/wfqtz4

### 6.9 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation (HSHQDC-17-R-00030) must be emailed to CSD-2017-BAA@hq.dhs.gov **no later than 4:30 PM EST on April 18, 2017**. Emails submitting questions are to include "Questions for IMPACT Research & Development BAA Solicitation" in the subject line. All questions and responses will be posted on the Federal Business Opportunities (FBO) website http://www.fbo.gov. **IMPORTANT NOTE--Questions will only be accepted and answered electronically.**

### 6.10 Order of Precedence

***Additional Information***: In the event that any of the terms and conditions contained in this solicitation (HSHQDC-17-R-00030) conflict with terms and conditions included in DHS/S&T/CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue), the terms and conditions in DHS/S&T/CSD 5-Year BAA HSHQDC-17-R-B0002 shall take precedence.

**REFERENCES:**

1. National Artificial Intelligence Research and Development Strategic Plan, October 2016, pp. 30-31. https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf
2. In 2016 IMPACT transitioned from PREDICT (Protected Repository for the Defense of Infrastructure against Cyber Threats), the original research infrastructure program implemented in 2004 as a direct response to the 2003 National Strategy to Secure Cyberspace, and later driven by the 2009 White House Cyberspace Policy Review. https://www.impactcybertrust.org/
3. National Critical Infrastructures Security and Resilience Research & Development Plan, November 2015, p. 17. https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf
4. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 35-36. https://www.federalregister.gov/documents/2015/04/27/2015-09697/request-for-information-rfi-federal-cybersecurity-randd-strategic-plan
5. Impact Cyber Trust, What We Do, https://www.impactcybertrust.org/what; Impact Cyber Trust, Legal Tools, https://www.impactcybertrust.org/tools_legal
6. Homeland Security Enterprise is defined as the broad scope of contributions from all federal agencies, levels of governments, businesses, and nongovernmental organizations, individuals, families, and communities, as well as international partnerships. https://www.dhs.gov/homeland-security-enterprise
7. Federal Cyber Security Research and Development Strategic Plan, February 2016, pp 30, 44. https://www.federalregister.gov/documents/2015/04/27/2015-09697/request-for-information-rfi-federal-cybersecurity-randd-strategic-plan
8. Science and Technology Directorate Strategic Plan 2015-2019, p.36. https://www.dhs.gov/sites/default/files/publications/st/ST_Strategic_Plan_2015_508.pdf
9. National Critical Infrastructures Security and Resilience R&D Plan, November 2015, p. 19. https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf
10. National Critical Infrastructures Security and Resilience R&D Plan, November 2015, p. 16. https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf
11. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 35. https://www.federalregister.gov/documents/2015/04/27/2015-09697/request-for-information-rfi-federal-cybersecurity-randd-strategic-plan
12. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 17. https://www.federalregister.gov/documents/2015/04/27/2015-09697/request-for-information-rfi-federal-cybersecurity-randd-strategic-plan
13. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 17, 24. https://www.federalregister.gov/documents/2015/04/27/2015-09697/request-for-information-rfi-federal-cybersecurity-randd-strategic-plan
14. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 35. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf
15. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 41. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf
16. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 49. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

17. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 30. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf
18. DHS 2014 Quadrennial Homeland Security Review, June 2014, p. 55. https://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf
19. Impact Cyber Trust, What We Do https://www.impactcybertrust.org/what
20. Camp, J., Cranor, L., Feamster, N., Feigenbaum, J., Forrest, S., Kotz, D., ... & Rivest, R. (2009). Data for cybersecurity research: Process and "wish list".
21. CSD Projects https://www.dhs.gov/science-and-technology/csd-projects
22. Federal Cyber Security Research and Development Strategic Plan, February 2016, p. 35 https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf
23. Capabilities DO NOT include the development and deployment of platforms for distributed query-response for operational, real-time sharing of tactical threat intelligence.

# Appendix A: IMPACT BAA Model

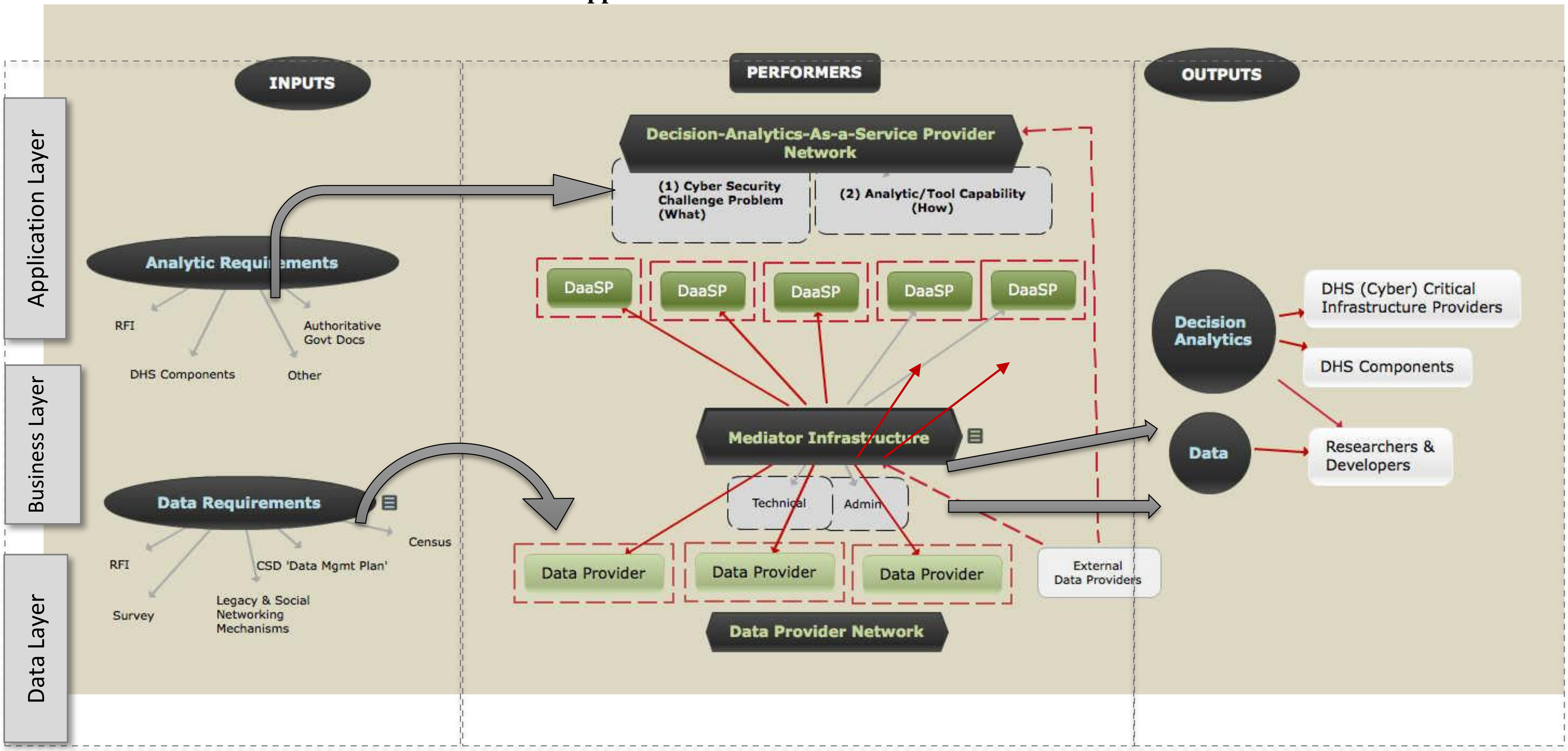


**DIAGRAM Legend: Next-Generation IMPACT DIMENSIONS: (1) Inputs:** Articulate target customer decision needs; **(2) Performers:** Specify how #1 Inputs will be addressed: translate into Cyber Security Challenge Problem(s) addressed, and the foundational data and analytical environment design to enable the (**3) Outputs:** Analytics and Data used by target customers, which are also a basis to measure and improve the outcomes and value created from capability development in #2.